Wild Card

How Information Flows from the Modern Battlefield

By John W. Davis

Imagine the horror of death by friendly fire. See the faces of a mother and father at the moment they are told their son or daughter was killed by American fire. Today, far more than bullets can cause this horrific scene. This is a new age and there are new threats.

Information warfare is the latest theme to capture the imagination of the U.S. Army. The Objective Force, the technological army with the narrow soldier base, depends on the rapid and accurate flow of information to fuel its highly technical killing power. To protect its classified information, this army can depend on traditional security elements. This new army, however, also generates a massive amount of unclassified material that is overlooked by traditional security measures. Could this material reveal the secrets the Army hopes to protect? In the information revolution, "open source" information is the wild card of the modern battlefield. It is a form of friendly fire. The Army must protect this vulnerability through operations security.

Information — its access, use, analysis, and control — is clearly a military matter. Classified information is protected by an array of security measures that are well known and practiced. But what about the literally millions of bits of unclassified personnel, logistical, operational, and supply documents that the Objective Force is generating? What can this information reveal and who will watch over it? What will protect this information that spews out over unsecured faxes, e-mail messages and telephone networks?

"The General is skillful in attack whose opponent does not know what to defend, and he is skillful in defense whose opponent does not know what to attack."

— Sun Tsu 400-321 B.C

In the furor over recent revelations of Chinese espionage, who has asked how much they gathered from totally legal, totally open sources? What country will risk a major espionage recruitment when the same materials could be collected from an uncontrolled, open military Web site? Was it not Mao Tse Tung himself who counseled that, "The commander applies all possible and necessary methods of reconnaissance and ponders on the information gathered, eliminating the false and retaining the true, proceeding from one to the other, from the outside to the inside…?" Does this not suggest collecting the unclassified until one can interpolate the secret?

The Army must face this modern problem. Can the flow of information necessary to conduct operations hurt the Service? What if the unclassified material is so voluminous, so comprehensive that it reveals the essential secrets the Army is otherwise so careful to protect?

At the beginning of World War II, some 300 British engineers died because they could not defuse the new electrical bombs dropped by the Germans over England. It took trial and error and the chance discovery of intact electrical bombs on a downed German aircraft before the technology was defeated.

Eight years earlier, in 1932, the technology for such bombs had been entered into the public records of the British patent office, yet none of the engineers knew about this open source of information.

Three hundred men died while the answer they sought gathered dust in an unlikely place. Those who built the bombs that killed these men had found the information first and laid claim to it legally and openly. Had they known this, it would have been easy to convince the British people of the value of open source awareness.

A shop-worn story of yesteryear? Are hired workers on NATO compounds in the Balkans pacing off mortar ranges, as did the Vietnamese before them? Was it not the Belgian resistance fighter who said that people who experience occupation know the adversary better than he knows himself?

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Wild Card. How Information Flows from the Modern Battlefield	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Space & Missile Defense Command,Army Forces Strategic Command,Redstone Arsenal,AL,35809**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

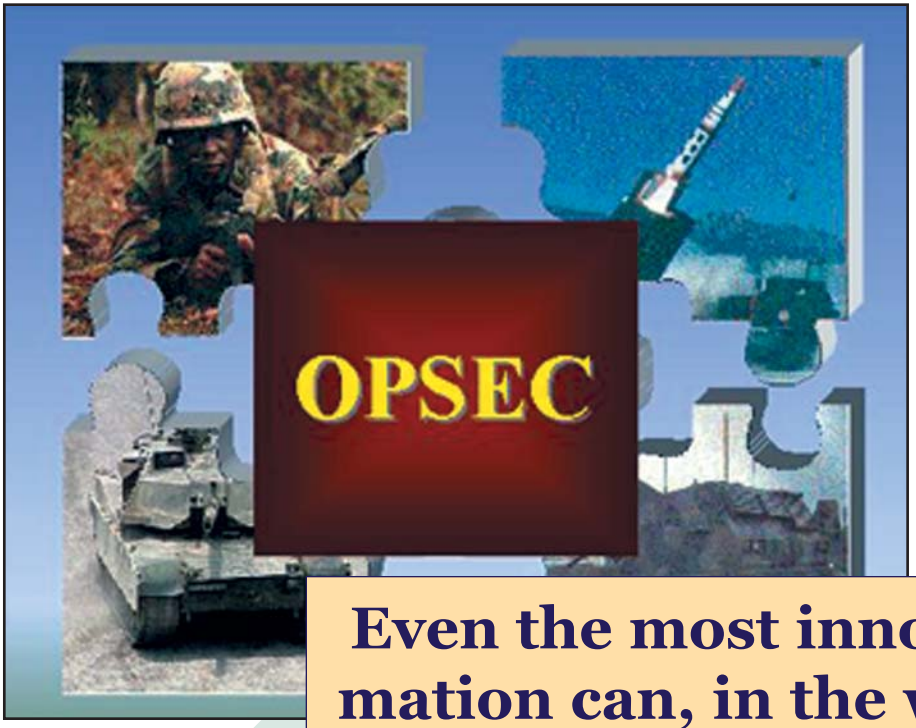
12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**4**	



Even the most innocuous information can, in the wrong hands, kill

The arms race fuels the West's ever expanding market and the information-rich marketing ethic that advertises it. The military must create policies that protect all its information — even the unclassified — because, in this new world, information that kills soldiers is a commodity available for sale.

Operations security, a process of securing this unclassified information, can protect the Objective Force. The security process is simple. Each element of the Army must ask itself, "What is it that I must protect, or else I'll fail in my mission?" The answer is that critical information must be protected. Not everything that can compromise a mission is classified.

An earlier example involves the Maxim gun. When asked in 1884 why Western nations had colonized almost the entire known world, the English writer Hilaire Belloc said that it was not because of their advanced civilization, greater universities, or cultural advances.

No, he quipped, "Whatever happens, we have got the Maxim gun, and they have not!" Of course, the technology for this early machine gun and other technological information was routinely shared and sold in open contracts between "civilized" countries. In World War I this exchange of information resulted in the slaughter of an entire generation; by then all nations had access to the Maxim gun.

These stories show how open source, openly available information works. What is routinely, even inadvertently given away today could kill someone tomorrow. Information that is not tracked could later surprise the Army on the battlefield. These stories about open source information end in bloodshed. Is it inappropriate to say that the victims died from friendly fire?

Information is the lifeblood of the high-technology Objective Force. An array of information will deploy with the Objective Force wherever it goes, whoever the adversary is. Unlike most of the adversaries of the United States, whose technological developments are not shared openly, much of the information about the Objective Forces' development is available to the entire world. For example, the Associated Press reported on a Pentagon armaments display showing soldiers with heat-sensitive night-vision sight, lightweight body armor, and computer backpacks. They reported concepts about laser warplanes, seagoing missiles, and more. Today there are many armaments magazines, defense sites on the Internet, and newspapers reporting the business of warfare. These open sources of information are cheap, readily accessible, and accurate.

Through the eyes of a Western analyst, the publications are what they seem: military trade journals that cover market share, sales opportunities, competitive and joint ventures, and national acquisition goals. They are straightforward.

Graphs and computer-generated art enhance the stories and illustrate the concepts. In the photographs used, sleek missiles fly, spotless armored vehicles roll, and wholesome, clean soldiers pose with the latest weaponry in pleasant pastures. There is no blood.

Consider now the reader of this same information from poorer, less industrialized, embargoed, or otherwise ostracized nations. Consider also the people of paranations, the ethnic clans, narcotics traffickers, and terrorists. They see the same information in terms of life or death choices. They cannot afford technical research or development, and they cannot "comparison shop." They

(See Wild Card, page 54)

know they must choose wisely the first time because there may not be a second choice. For them, the only collection method may be what they can learn from open publications. The more sophisticated groups can build on information from open sources and confirm their conclusions with traditional collection methods. Their interest is far from abstract.

Several truisms must be accepted in this new world of half-wars against nontraditional adversaries. Poorer nations want to survive. In order to do so they are offered the Hobson's choice of spending what wealth they have on arms or relying on a guardian nation to arm their people. They are not interested in future sales, in market share, or in the bottom line. If they do not choose correctly from the arms necessary to protect themselves, they will cease to exist, or worse, be enslaved. Obviously, they see the world from a dramatically different perspective.

The West views military technology as a chess game. One player creates this, the opponent creates that to counter it, and so on. In this rational game of give and take, no one dies and the game goes on. Some call this the arms race, but nobody dies in a race. Such a sterile view of the industry misses the point.

Analysts of arms markets from non-Western countries or para-nations see the armaments industry differently and arguably more clearly than Western nations do. They, like the United States, will determine their needs and do all within their power and budget to acquire those necessities. Unlike the United States, they see their existence as often nasty, brutish, and short. They often feel they must confront the killer at the door, rather than the economic competitor in the pinstriped suit. It is not surprising that poorer countries decided to buy machine guns as soon as they could afford them, once they saw what happened to those who did not.

The callousness of the Western businessman who commented about a recent technology theft, "Who cares, we'll just build a counter-measure," would be incomprehensible to his counterparts in a poorer country who bet their very existence on successfully using proven technology in the near term.

Those of poorer countries have a vested interest in what is available on the arms market today, and in knowing how their potential adversary will fight. What if their potential adversary is the United States?

These poorer countries want to know, simply put, how to beat the United States in battle. To be able to surprise the U.S. military, they will try to learn more about it than the military knows about itself. They do not have the wherewithal to conduct massive technical research, so they will take any shortcut. All open sources will be exploited. Why spend the money on research and development if the final product is going to be for sale or is explained on the Internet? Why test weapons if the answers nations seek are printed in publications that cost only a few dollars each? Comparison tests will be done by those governments that see weaponry more as a commodity to be marketed than as a means of killing people.

Western powers think of long-term strategies while poorer nations wonder how to stop the immediate threat. They know they are dead if they make the wrong choices, so they research information thoroughly. If they can piece together information about the true intentions of an adversary from what they can collect on the open source market, they will do so. It may be the only source they have. These are the types of adversaries the U.S. military will confront tomorrow.

These differing perceptions of the world — one by rich nations, the other by poor — must be better understood. A poor man does not care about higher technology tomorrow if his weapon will surprise his enemy today. To achieve this he may act in a way contrary to what the West considers being in his best, rational interest. Westerners must see the world with new eyes — their potential adversary's eyes. History offers many examples.

In the 1920s, for instance, a beaten Germany, penned in by the Treaty of Versailles, entered joint ventures with Bofors Corp. of neutral Sweden. The Germans had studied the published armament policies of other European nations and had observed the soldiers occupying their country. They had studied what would win on a future battlefield, then set out to get it any way they could.

Before World War II, Germany illegally trained its army on the land of its arch-rival, the Soviet Union. Despite open reports of Germany's illicit training, other nations were too complacent to challenge this threat. The West was thinking about long-term, rational arms races. Germany was thinking about a blitzkrieg.

In a later example, the United States was shocked when it was revealed that the Vietnamese communists had routinely spliced into U.S. telephone lines. Open communications were compromised. These were simple farmers who should not have had the capability, the United States complained. The nation did not see the world through its adversary's eyes.

Today, are the Afghani or Iraqi government troops trained by the U.S. going to rest assured that the West will protect them? Did the Serbs or Muslims rely on the United States or NATO to take action against a vengeful adversary, or did they take their own measures? Does anyone doubt, however, that they are devouring every statement and operational move we make in our many deployments?

Every document, every communication made by the U.S. military's soldiers is subject to collection. Seemingly innocent communications could confirm or deny the fears of the many groups involved in Afghanistan, Iraq, Kosovo or Bosnia. How many American soldiers realize that a TDY order, supply form, or logistical document could betray the military's true intentions? Open source information takes this operational release of information even farther.

Westerners may see no great loss when technology is compromised because they may never see the battlefield result of their work. They may think abstractly of their product as a funded program, not as something that kills someone. Their counterparts in another, less powerful country would face imprisonment or execution if they compromised hard-gathered information.

Westerners must "publish or perish." They have a "right to know" and a free and inquisitive press. Non-Western counterparts do not.

Next, the collection threat to this critical information must be studied. Soldiers must consider who wants what they have. Here, the intelligence community can provide assistance. The collection capability could be a highly sophisticated process or a hacker who can read the Army's e-mail. In weighing the threat to the critical information, the answer to the next question, "Is the Army vulnerable?" may be surprising. Even units with 100 percent traditional security of their classified information have been compromised by a hemorrhage of unclassified data. Unit leaders did not tell their soldiers what was critical to protect, and soldiers did not control bar talk, telephone talk, or what went out over the wire, much less what went into the trash. After the risks are weighed, such as collection capabilities and reaction times, countermeasures must be decided on.

The Army must communicate to accomplish any mission, but it has to remain aware of the unseen listener. Soldiers must know what an adversary can do. To survive, other countries will read everything the Army writes and listen to any conversation they can. The Army has to see itself as others see it.

Once they learned that the Viet Cong had made tiny mines from discarded C-ration cans, soldiers stopped leaving cans uncontrolled. Now, the Army should do no less with its open source information.

John W. Davis, a retired U.S. Army MAJ, teaches the threat portions of the Department of the Army's Operations Security course at the Space and Missile Defense Command, Huntsville, AL.